



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/396,054	09/15/1999	YOSHIHITO ISHIBASHI	450100-02090	6914

20999 7590 03/05/2004
FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER

ABEL JALIL, NEVEEN

ART UNIT	PAPER NUMBER
----------	--------------

2175

DATE MAILED: 03/05/2004

9

Please find below and/or attached an Office communication concerning this application or proceeding.

3

Office Action Summary

Application No.

09/396,054

Applicant(s)

ISHIBASHI, YOSHIHITO

Examiner

Neveen Abel-Jalil

Art Unit

2175

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on January 2, 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-41 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The amendment filed on January 2, 2004 has been received and entered. Claims 1-41 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

3. Claims 1-41 are rejected under 35 U.S.C. 102(e) as being anticipated by Shimizu et al. (U.S. Patent No. 6,085,323).

As to claim 1, Shimizu et al. discloses a content management method for a data storage provided with a plurality of content storing means (See column 1, lines 66-67), comprising the steps of:

Art Unit: 2175

decrypting, with a first storage key, a content key encrypted with the first storage key and stored along with a content encrypted with the content key in a first content storing means (See column 4, lines 34-55);

encrypting the content key obtained by the above decryption with a newly generated second storage key (See column 3, lines 6-40); and

storing the content key encrypted with the second storage key along with the encrypted content in a second content storing means (See column 3, lines 59-66).

whereby said first and second content storing means are located at a site that is remote from the site where said encrypting is performed (See column 12, lines 38-45, also see column 13, lines 6-14, and see column 1, lines 48-67, and see figure 39, 605, shows "contents" being remote from 601, "decoder", also see column 1, lines 23-32).

As to claim 2, Shimizu et al. discloses wherein the second storage key is generated based on a random number (See column 7, lines 53-55, also see column 12, lines 46-57).

As to claim 3, Shimizu et al. discloses wherein the content key obtained by the decryption is encrypted with identification information of the second content storing means and stored into the second content storing means (See column 3, lines 59-66, also see column 13, lines 15-25).

As to claim 4, Shimizu et al. discloses wherein the content key is encrypted, in the first content storing means, with the first storage key and identification information of the first

Art Unit: 2175

content storing means, and the content key stored in the first content storing means is decrypted with the first storage key and identification information of the first content storing means (See column 2, lines 48-65).

As to claim 5, Shimizu et al. discloses wherein the second storage key is generated by a decrypted key generating means provided in the data storage (See column 3, lines 6-35).

As to claim 6, Shimizu et al. discloses wherein the second storage key is encrypted with a public key for a key management unit for management of the storage keys to generate a third storage key and the third storage key is stored into the second content storing means (See column 7, lines 4-49, and see column 8, lines 19-33).

As to claim 7, Shimizu et al. discloses wherein the data storage deletes the second storage key depending upon whether the third storage key has been stored in the second content storing means (See column 24, lines 43-50).

As to claim 8, Shimizu et al. discloses wherein when decrypting the content key stored in the second content storing means, the data storage sends the third storage key to the key management unit; and the key management unit generates a second storage key based on the third storage key while accounting the data service following a predetermined procedure (See column 10, lines 61-67, and column 11, lines 1-10, wherein “third key” reads on “temporary key”).

As to claim 9, Shimizu et al. discloses wherein the second storage key is generated by a storage key generating means provided in the key management unit which manages the storage keys; and the key management unit has stored therein the second storage key and the identification information of the second content storing means in which the content key encrypted with the above generated second storage key (See column 4, lines 14-33).

As to claim 10, Shimizu et al. discloses wherein upon the generation of the second storage key, the key management unit accounts the data service following the predetermined procedure (See column 11, lines 1-25, also see column 19, lines 8-21)

As to claim 11, Shimizu et al. discloses wherein the key management unit (See column 13, lines 6-25) encrypts the second storage key with the management key to generate a third storage key, and sends the third storage key to the data storage (See column 25, lines 10-22, also see column 26, lines 52-55); and

the data storage stores the received third storage key into the second content storing means (See column 9, lines 20-32).

As to claim 12, Shimizu et al. discloses wherein the data storage deletes the second storage key depending upon whether the third storage key has been stored in the second content storing means (See column 20, lines 26-32, also see column

Art Unit: 2175

As to claim 13, Shimizu et al. discloses wherein the key management unit has stored therein the identification information of the second content storing means in which the content key encrypted with the second storage key; the data storage sends, when decrypting the content key stored in the second content storing means, the identification information of the second content storing means to the key management unit (See column 2, lines 59-65, also see column 13, lines 15-25, also see column 24, lines 43-49); and

the key management unit generates a second storage key based on the result of comparison between the identification information of the second content storing means, send from the data storage, and the identification information of the second content storing means, held in the key management unit itself, while accounting the data service following the predetermined procedure (See column 9, lines 65-67, and column 10, lines 1-30).

As to claim 14, Shimizu et al. discloses wherein the second content storing means has stored therein the identification information of the data storage (See column 10, lines 19-30, also see column 2, lines 59-65).

As to claim 15, Shimizu et al. discloses wherein the data storage starts decrypting the content key stored in the second content storing means depending upon the result of an inspection of the identification information of the data storage, stored in the second content storing means (See column 10, lines 1-50).

Art Unit: 2175

As to claim 16, Shimizu et al. discloses wherein the decrypted content key supplied from the second content storing means has added thereto information that the content key is a one obtained by restoration (See column 15, lines 13-48, also see column 16, lines 25-34).

As to claim 17, Shimizu et al. discloses wherein when moving the content key having added thereto the information that the content key is a restored one, the data storage makes an error process based on the result of comparison between the content key and a content key stored in a destination to which the content key is to be moved (See column 23, lines 15-49).

As to claim 18, Shimizu et al. discloses wherein the content key has added thereto frequency information which limits the number of times the content key can be used (See column 15, lines 28-35, also see column 15, lines 49-52).

As to claim 19, Shimizu et al. discloses wherein the content key stored in the first content storing means is stored along with the identification information of the first content storing means into the second content storing means; the identification information stored in the second content storing means is stored into the data storage when the content key stored in the second content storing means is decrypted (See column 20, lines 27-67, also see column 24, lines 43-49, also see column 10, lines 19-30); and

the data storage makes, when a request is made to decrypt the content key in the first content storing means, an error process based on the result of comparison between the identification information of the first content storing means in consideration and the

Art Unit: 2175

identification information of the second content storing means (See column 9, lines 48-64, also see column 10, lines 7-30).

As to claim 20, Shimizu et al. discloses a content storage system, comprising:

a first content storing means having stored therein a content key encrypted with a first storage key and a content encrypted with the content key (See column 24, lines 57-67, and see column 25, lines 1-7);

means for decrypting a data and key data;

means for encrypting the data and key data;

means for generating a storage key (See column 24, lines 23-39);

a second content storing means for storing an encrypted content key obtained by encrypting, in the encrypting means, the content key obtained by decryption with the first storage key in the decrypting means, using the second storage key generated by the storage key generating means, and the encrypted content; and

means for storing the storage keys (See column 3, lines 6-22).

whereby said first and second content storing means are located at a site that is remote from the site where said encrypting is performed (See column 12, lines 38-45, also see column 13, lines 6-14, and see column 1, lines 48-67, and see figure 39, 605, shows "contents" being remote from 601, "decoder", also see column 1, lines 23-32).

Art Unit: 2175

As to claim 21, Shimizu et al. discloses wherein the storage key storing means generates the second storage key by means of a random number generator (See column 7, lines 53-55, also see column 12, lines 46-57).

As to claim 22, Shimizu et al. discloses wherein a content key obtained by encrypting, in the encrypting means, the content key obtained by the decryption in the decrypting means, with the first storage key and identification information of the second content storing means, is stored in the second content storing means (See column 10, lines 61-67, and see column 11, lines 6, also see column 24, lines 50-66).

As to claim 23, Shimizu et al. discloses wherein the content key is encrypted, in the first content storing means, with the first storage key and identification information of the first content storing means; and the content key stored in the first content storing means is decrypted with the first storage key and identification information of the first content storing means (See column 2, lines 48-65).

As to claim 24, Shimizu et al. discloses wherein the first content storing means, decrypting means, encrypting means, second content storing means, storage key storing means and storage key generating means form together a data storage (See column 2, lines 49-65); and further comprising a key management unit which manages the storage keys of the data storage (See column 13, lines 15-25).

Art Unit: 2175

As to claim 25, Shimizu et al. discloses wherein the data storage is a data receiver which receives a content encrypted and sent from a data transmitter (See column 1, lines 60-67, also see column 12, lines 40-45, also see column 26, lines 36-49).

As to claim 26, Shimizu et al. discloses comprising means for storing the public key of the key management unit; and wherein the second content storing means has stored therein the second storage key along with a third storage key obtained by encrypting the second storage key with the public key (See column 19, lines 53-67, also see column 9, lines 20-47, wherein “third key” reads on “temporary key”).

As to claim 27, Shimizu et al. discloses wherein the data storage deletes the second storage key depending upon whether the third storage key is stored in the second content storing means (See column 24, lines 43-50).

As to claim 28, Shimizu et al. discloses wherein when decrypting the content key stored in the second content storing means, the data storage sends the third storage key to the key management unit; and the key management unit sends a second storage key generated based on the third storage key to the data transmitter while accounting the data service following a predetermined procedure (See column 11, lines 11-45).

As to claim 29, Shimizu et al. discloses wherein the second content storing means has stored therein the identification information of the data storage (See column 14, lines 22-52).

As to claim 30, Shimizu et al. discloses wherein the data storage starts decrypting the content key stored in the second content storing means depending on the result of inspection of the identification information of the data storage, stored in the second content storing means (See column 10, lines 1-50).

As to claim 31, Shimizu et al. discloses wherein the first content storing means, decrypting means, encrypting means, second content storing means and storage key storing means form together a data storage (See column 2, lines 49-65); and comprising the storage key generating means and further a key management unit which manages the storage keys of the data storage (See column 13, lines 15-25).

As to claim 32, Shimizu et al. discloses wherein the data storage is a data receiver which receives a content encrypted and sent from a data transmitter (See column 1, lines 60-67, also see column 12, lines 40-45, also see column 26, lines 36-49).

As to claim 33, Shimizu et al. discloses wherein the key management unit comprises an identification information storing means in which the storage key generated by the key management unit and the identification information of the content storing means in which the content key encrypted with the generated storage key (See column 25, lines 10-23, also see column 13, lines 15-25).

As to claim 34, Shimizu et al. discloses wherein the key management unit accounts the data service following the predetermined procedure depending upon the generation of the storage key (See column 12, lines 40-62).

As to claim 35, Shimizu et al. discloses wherein the key management unit comprises means for storing storage keys (See column 13, lines 6-25);

the key management unit generates a third storage key by decrypting the second storage key with the storage key and sends it to the data storage (See column 25, lines 10-22, also see column 26, lines 52-55); and

the data storage stores the third storage key into the second content storing means (See column 9, lines 20-32).

As to claim 36, Shimizu et al. discloses wherein the data storage deletes the second storage key depending upon whether the third storage key is stored into the second content storing means (See column 4, lines 34-55).

As to claim 37, Shimizu et al. discloses wherein the key management unit comprises means for storing the second storage key and the identification information of the second content storing means in which the content key encrypted with the second storage key is stored (See column 2, lines 60-65, also see column 24, lines 57-67, and see column 25, lines 1-7);

the key management unit accounts, when the data storage decrypts the content key, the data service following the predetermined procedure based on the result of comparison between

Art Unit: 2175

the identification information of the second content storing means, sent from the data storage, and the identification information stored in the identification information storing means (See column 10, lines 1-50).

As to claim 38, Shimizu et al. discloses wherein the second content storing means has stored therein the identification information of the data storage (See column 14, lines 22-52).

As to claim 39, Shimizu et al. discloses wherein the data storage starts decrypting the content key stored in the second content storing means (See column 11, lines 1-30).

As to claim 40, Shimizu et al. discloses wherein the content key obtained by decryption from the second content storing means has added thereto information that the content key is a one obtained by restoration, as requirement information (See column 15, lines 13-48, also see column 16, lines 25-34).

As to claim 41, Shimizu et al. discloses wherein the content key has added thereto frequency information which limits the number of times the content key can be used (See column 12, lines 46-57, also see column 10, lines 8-18).

Response to Arguments

4. Applicant's arguments filed on January 2, 2004 have been fully considered but they are not persuasive.

Art Unit: 2175

Applicant's argument that "Shimizu fails to disclose a storage scheme in which data is stored in first and second content storing means wherein key data is encrypted and stored in the second content means and wherein the first and second content storing means are located at a site that is remote from the site where the encryption is performed" is respectfully acknowledged but is not deemed to be persuasive.

The Examiner respectfully points to Shimizu abstract and column 12, lines 38-45, also see column 13, lines 6-14, and see column 1, lines 48-67, and see figure 39, 605, shows "contents" being remote from 601, "decoder", also see column 1, lines 23-32, where Shimizu talks about the data encrypted being stored on a remote computer away from the portable computer the focus of the his invention where the encryption takes place before transmitting or receiving data from a LAN or remotely connected shared computer. Shimizu clearly teaches that the methods of his invention are operable on portable computer that receives third party access to stored information and can request/ receive information as the encryption object from a different device. As it is well known in the art, any content prior or after encryption can be stored internally or remotely on a device.

Conclusion

5. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

Art Unit: 2175


MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Neveen Abel-Jalil whose telephone number is 703-305-8114. The examiner can normally be reached on 8:00AM-4: 30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on 703-305-3830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Neveen Abel-Jalil
March 2, 2004


CHARLES RONES
PRIMARY EXAMINER